Department of Homeland Security
IAIP Directorate
Daily Open Source Infrastructure Report
for 15 June 2004

Current Nationwide Threat Level is
ELEVATED
Significant Risk of Terrorist Attacks
For info click here
www.whitehouse.gov/homeland

Daily Overview

- The Poughkeepsie Journal reports a water system that serves the Town of Wappinger, NY, was closed after a gasoline spill threatened to contaminate the water supply. (See item 17)
- CIDRAP News reports the Centers for Disease Control and Prevention has published a guidebook to help medical examiners and coroners detect and respond to bioterrorism. (See item 20)
- Reuters reports Nuradin Abdi, a Somali man living in Ohio, has been charged with conspiracy to provide material support to al Qaeda in a plot to blow up a shopping mall in Columbus. (See item 27)

Energy Sector

Current Electricity Sector Threat Alert Levels: Physical: Elevated, Cyber: Elevated
Scale: LOW, GUARDED, ELEVATED, HIGH, SEVERE [Source: ISAC for the Electricity Sector (ES−ISAC) − http://esisac.com]

1. *June 14, Associated Press* — **Power outages reportedly linked to distribution problem at Palo Verde. A disruption in the power grid system serving Arizona caused thousands of Arizonans to lose power on Monday, June 14. The outages affected about 35,000 Tucson Electric Power customers in the Tucson area and 30,000 Arizona Public Service (APS) customers on the Phoenix metro area's west and northwest sides.** APS spokesperson Jim McDonald says the disruption in the power grid occurred at 7:41 a.m. and lasted for less than an hour. Arcing power lines due to the disruption also caused some small brush fires in Peoria that

were quickly controlled. The disruption caused all three units at the Palo Verde nuclear power plant to shut down, as APS says they are designed to do. Two units at APS's Redhawk power plant also shut down. APS says it has adequate power to service its customers despite the shut−downs.
Source: http://kvoa.com/Global/story.asp?S=1939659&nav=HMO5NtcC

2. *June 14, Click2Houston.com* — **Man on transmission tower disrupts traffic. A man climbed a 345,000−volt transmission tower in southwest Houston, TX, on Monday, June 14, forcing police to close a nearby toll way. CenterPoint Energy officials cut electricity to that tower, but said nearby homes and businesses were not affected.** Police have tried to convince the man to come down. Officers are using a bullhorn to communicate with him, but the man has not said anything. Police feared the man was going to jump for a while due to the way he was standing. He has also spent part of the time sitting down. The unidentified man has pulled his shirt over his face so he would not be recognized.
Source: http://www.click2houston.com/news/3416568/detail.html

[Return to top]

Chemical Industry and Hazardous Materials Sector

Nothing to report.
[Return to top]

Defense Industrial Base Sector

3. *June 14, Washington Post* — **Updated computers for the B−52.** A private contractor won a $30 million contract to deliver new computers for the aging B−52 bomber that will enable the Air Force to continue flying the plane until 2050. The bomber's latest computers will give it the ability to carry more types of weapons, said Louis DeSantis, a vice president at the private contractor overseeing the contract. The contractor declined to give more details about the bomber's future capabilities, but the plane's greater flexibility is part of the Pentagon's efforts to make the military lighter and faster. The new computers are the first replacements for the bomber's original computers. Faster, more powerful and with lots more memory, two of the new computers will replace four old computers on each bomber. **The new computers will allow the aircraft to give up its reliance on the custom−built software now running the electronic insides of the bomber and instead take advantage of standardized software sold by private companies. The contractor said it expects to begin installing the computers next year and complete the work by 2009.**
Source: http://www.washingtonpost.com/wp−dyn/articles/A38995−2004Jun 13.html

4. *June 11, National Journal's Technology Daily* — **Department of Defense drafts stronger software security rules. Stiffer requirements for the security of software purchased by the Department of Defense (DoD) should be in place by the end of next year, according to a department official. DoD, the Department of Homeland Security and other federal entities are working actively this summer to develop a way to extend current software certification procedures to be able to exclude products and services or companies deemed**

too risky. Joe Jarzombek, a deputy director for software assurance at Defense's networks and information integration office, said current certification focuses on ensuring that the products do what they were billed to do. Now they will look for bad actors associated with the product or company, secure business practices and an evaluation of the product. Jarzombek said the department recognizes it cannot currently address all existing cybersecurity threats, even as it moves all operations and functions into an Internet−based environment, a process referred to as "network centricity." The department calculates that the cost of reacting to cyber attacks is far greater than the cost of preventing them, he said. Ninety percent of attacks are against known vulnerabilities, and the cost is between $1 million and $4 million per patch.
Source: http://www.govexec.com/dailyfed/0604/061104tdpm1.htm

[Return to top]

Banking and Finance Sector

5. *June 14, Reuters* — **Wintrust to buy Wisconsin bank Town Bankshares. Wintrust Financial Corp., an Illinois banking company, on Monday, June 14, said it agreed to buy privately held Town Bankshares Ltd. for about $38.5 million in cash and stock to expand in Wisconsin.** Wintrust, based in Lake Forest, IL, said it will pay about $129.10 per share for Town, which had 298,206 shares outstanding as of March 31. Wintrust said the purchase is not expected to materially affect 2004 earnings per share and is expected to close early in the fourth quarter. The company on May 10 agreed to buy privately held Northview Financial Corp. for about $45.6 million to expand in suburban Chicago, IL. Wintrust has about $5 billion of assets and 41 banking offices. Town has about $232 million of assets.
Source: http://biz.yahoo.com/rc/040614/financial_wintrust_1.html

6. *June 14, Reuters* — **Sterling Financial to buy Pennsylvania State Banking. Sterling Financial Corp., a Pennsylvania bank, on Monday, June 14, said it agreed to buy Pennsylvania State Banking Co. for about $44 million in cash and stock, adding six branches in Cumberland and Dauphin counties.** Sterling, based in Lancaster, PA, as of March 31 had $2.34 billion of assets, and operates 56 banking offices in Pennsylvania, Delaware and Maryland. Pennslyvania State Banking, based in Camp Hill, PA, as of March 31 had $201 million of assets. The merger is expected to close in late 2004 or early 2005.
Source: http://biz.yahoo.com/rc/040614/financial_pennsylvaniastateba nking_1.html

7. *June 14, The Korea Times* — **Asia and pacific leaders to tackle money laundering.** About 300 representatives from throughout the Asia−Pacific region gathered in Seoul, South Korea, on Monday, June 14, for a five−day meeting to establish common ground on how to fight money laundering. **The participants from the 26 member countries of the Asia−Pacific Group on Money Laundering (APG) will seek ways of establishing international standards and evaluating their effectiveness.** At the Seoul meeting, Cambodia and Mongolia will join the group, which will increase total membership to 28. As a sideline to the meeting, the KFIU will sign memorandums of understanding with its Thai and Philippine counterparts on Wednesday, June 16, to broaden South Korea's ability to exchange information on cross−border money laundering practices. South Korea currently has similar MOUs with twelve countries.
Source: http://times.hankooki.com/lpage/200406/kt2004061414543712070 .htm

[Return to top]

Transportation Sector

8. *June 14, Department of Transportation* — **NHTSA proposes requirements for voluntarily installed event data recorders. The National Highway Traffic Safety Administration (NHTSA) on Monday, June 14, proposed standard requirements for Event Data Recorders (EDR) that manufacturers choose to install in light vehicles.** The proposed rule would not require the installation of EDRs. “EDRs are in most new vehicles and are already providing valuable safety information for our crash investigators and researchers,” said NHTSA Administrator Jeffrey W. Runge, M.D. NHTSA is proposing, beginning in September 2008, to: (1) require that the EDRs voluntarily installed in light vehicles record a minimum set of specified data elements useful for crash investigations; (2) specify requirements for that data; (3) increase the survivability of the EDRs and their data by requiring that they function during and after front, side and rear crash tests; (4) require vehicle manufacturers to make publicly available information that would enable crash investigators to retrieve data from the EDR; and (5) require vehicle manufacturers to include a brief, standardized statement in the owner’s manual indicating that the vehicle is equipped with an EDR and describing the purposes of EDRs. **An EDR is an electronic device that detects a crash and records certain information for several seconds of time before, during and after a crash.**
   Source: http://www.dot.gov/affairs/nhtsa2704.htm

9. *June 14, Department of Transportation* — **Investment in Seattle’s transportation future. Seattle is winning the battle against gridlock with the help of a $43.2 million grant announced on Monday, June 14, by U.S Federal Transit Administrator Jennifer L. Dorn. The grant to Sound Transit is for the continued construction a light rail line from downtown Seattle to Tukwila.** "A good transit investment keeps giving back to the community for decades to come," Administrator Dorn said as she announced the grant to members of the Sound Transit Board of Directors. Dorn told an audience gathered at Sound Transit’s Operations and Maintenance Facility that the Central Link Light Rail Transit Project will support Seattle's economic growth by “easing congestion, increasing mobility and enhancing the livability of this world−class city.”
   Source: http://www.dot.gov/affairs/fta1804.htm

10. *June 14, Federal Computer Week* — **E911 speeds BART calls. A new computer−based 911 call management system has cut the amount of time it takes San Francisco public transportation authorities to process calls to less than four seconds.** Using an Enhanced 911 solution, the San Francisco Bay Area Rapid Transit District (BART) reduced the handling time from 24 seconds. That might not seem like much, but it's significant during emergencies, officials said. BART officials process thousands of 911 calls across its 104−mile system from almost 1,000 pay phones, call boxes and private branch exchanges. **The full E911 rollout nationwide, coordinated by the Federal Communications Commission, is scheduled to be complete by December 31, 2005.** Many state and local agencies and telecommunication companies are struggling to meet this deadline.
    Source: http://www.fcw.com/fcw/articles/2004/0614/web−bart−06−14−04. asp

11. *June 14, Associated Press* — **FAA cuts distance between planes at O'Hare. The Federal Aviation Administration (FAA) will try to reduce flight delays at O'Hare International Airport by cutting in half the distance between planes landing and taking off on intersecting runways.** The plan will squeeze in about 10 more flights per hour into O'Hare when a certain combination of runways is used, officials said. "It will permit more flight operations while ensuring the same level of safety," FAA spokesman Tony Molinaro said. FAA officials developed the plan with American Airlines, United Airlines and pilot and controller unions. It was implemented Sunday, June 13. The plan is part of an ongoing effort by federal and local officials to reduce delays at the nation's most congested airport.
Source: http://www.usatoday.com/travel/news/2004−06−14−faa−ohare_x.h tm

[Return to top]

Postal and Shipping Sector

12. *June 13, Star−Ledger (NJ)* — **Mail delivered slowly to Congress. Letters and packages mailed to the Capitol can take longer than 10 days to arrive because of tightened security procedures following the anthrax attacks in 2001 and the February discovery of ricin in Senate Majority Leader Bill Frist's mailroom.** Normal delivery takes two to three days. Members say constituents should make greater use of e−mail, faxes, and the telephone to contact them. **Darius Goore, a spokesman for Sen. Jon Corzine (D−NJ), said the delivery time can sometimes stretch to "a couple of months."** Congressional aides say they now arrange for important overnight deliveries, magazines, and some newspapers to be sent to the homes of staff members or their lawmaker. Under the security procedures, letters and packages addressed to Washington ZIP codes for House and Senate offices, the White House, and 15 executive departments and agencies are collected each day in the nation's capital, then shipped 115 miles by truck up Interstate 95 to an irradiation plant. The U.S. Postal Service is now considering building its own, $9 million irradiation facility in the Washington, DC, area. The irradiated letters and packages irradiated are then sent to inspection facilities where workers open and inspect each piece of mail for biological and chemical agents. The mail also is screened for explosives.
Source: http://www.nj.com/news/ledger/index.ssf?/base/news−15/108710 9564209440.xml

[Return to top]

Agriculture Sector

13. *June 14, Fence Post (CO)* — **Animal response teams. The Colorado Veterinary Medical Foundation has decided to develop a State Animal Response Team (SART) in 2003, modeling the program after the North Carolina SART −− one of the first states to begin this work after experiencing hurricane devastation.** The premise behind SART programs is to address the issues of emergency situations that involve any animal, any disaster, anywhere in Colorado. The program will bring together a network of government agencies, not−for−profit organizations, animal industry professionals, and volunteers with the sole purpose of addressing animal emergency issues. According to Colorado SART there are over three million pet animals in the state and over seven million livestock. An animal emergency −− such as an

animal disease outbreak, whether unintentional or through bioterrorism −− could be devastating to the United States. These outbreaks can cause severe economic losses as well as threaten the safety of our food supply and our public health, especially if the disease is zoonotic, or a disease that can pass between human and animal. **Because many of the possible animal emergency situations need to be dealt with quickly, the core of Colorado SART are the County Animal Response Teams (CART), a network of people who can quickly assess a situation and act as soon as possible.**
Source: http://www.thefencepost.com/modules.php?op=modload&name=Submit_News&file=index

14. *June 14, just−food.com* — **Chiquita agrees to sell operations in Colombia. U.S. banana producer Chiquita Brands International has announced that it has entered into definitive agreements for the sale of its banana−producing and port operations in Colombia to Invesmar, the holding company of C.I. Banacol, a Colombia−based producer and exporter of bananas and other fruit products.** Under the terms of the deal Chiquita will receive around $28.5 million in cash and $15 million of notes and deferred payments for the operations, and the buyer will also assume around $8 million of pension liabilities. The transaction also includes two separate eight−year agreements for Chiquita's purchase from the buyer's affiliates of approximately 11 million boxes of Colombian bananas per year and approximately 2.5 million boxes of Costa Rican golden pineapples per year.
Source: http://www.just−food.com/news_detail.asp?art=57824

[Return to top]

Food Sector

15. *June 14, Wisconsin Ag Connection* — **Paprika recall. Brookfield, WI, based Penzeys Spices has expanded its recall of Hungarian Sweet Paprika, saying there is a possible salmonella contamination in its product. The company said last week that the recall involves all sizes of Hungarian Sweet Paprika distributed in early January through mail orders as well as in Penzeys Spices stores in 12 states.** The expanded recall comes weeks after Penzeys recalled packages of another paprika version, Hungarian Half−Sharp and some of its Hungarian Sweet Paprika, because of possible salmonella contamination. Health officials say young children, the elderly and people with weakened immune systems are especially vulnerable to infection from salmonella. However, the company said no reports of illness have been received. Routine testing by inspectors revealed salmonella in some jars of Hungarian Paprika, Penzeys said.
Source: http://www.wisconsinagconnection.com/story−state.cfm?Id=707& yr=2004

16. *June 10, Food and Drug Administration* — **Sprouts recalled. Sunshine Sprouts of Medford, OR, is recalling its Sunshine brand Alfalfa Sprouts and its Sunshine brand Spicy Sprout Mix because they have the potential to be contaminated with Salmonella bovismorbificans.** This organism can cause serious and sometimes fatal infections in young children, frail or elderly people, and others with weakened immune systems. In rare circumstances, infection with Salmonella can result in the organism getting into the bloodstream and producing more severe illnesses such as arterial infections, endocarditis, and arthritis. The Sunshine brand Alfalfa Sprouts and Sunshine brand Spicy Sprout Mix were distributed through retail stores in southern Oregon and northern California. **To date, one case**

of Salmonella Bovismorbificans possibly linked to the consumption of Sunshine brand raw alfalfa sprouts has been reported.
Source: http://www.fda.gov/oc/po/firmrecalls/sunshine06_04.html

[Return to top]

Water Sector

17. *June 11, Poughkeepsie Journal (NY)* — **Fuel spill closes water system. A water system that serves 5,000 Town of Wappinger, NY, homes was closed after a 12,000−gallon gasoline spill threatened to contaminate the water supply, Town Supervisor Joseph Ruggiero said.** About 12,000 people normally get drinking water from the Atlas Water District. The district's wells are about 4,500 feet from the spill. No contamination had yet reached the Atlas aquifer system, and no gasoline spilled directly into the nearby Wappinger Creek, Ruggiero said. The town's other water supply, the Hilltop well system, is adequate to supply the town's residents, but all are being asked to conserve water. The Hilltop system's capacity is about 1.4 million gallons per day. The town can consume 1.6 million on a typical summer day, Ruggiero said. The Atlas system has a one million gallon per day capacity.
Source: http://www.poughkeepsiejournal.com/news/update/061104.shtml

[Return to top]

Public Health Sector

18. *June 13, Scout News* — **Rapid SARS test.** China has given the green light for a new and simple test for Severe Acute Respiratory Sydrome (SARS) to go on sale, the official Xinhua news agency reports. **A state Food and Drug Administration official has told the agency that the test can detect SARS in patients between one to 10 days after they become ill, according to Agence France Presse.** Until now, it has taken health authorities weeks to confirm if a person has contracted SARS. Tests that detect SARS by establishing the presence of antibodies or the virus' nucleic acid are already on sale in China. The new test is relatively cheap and simple to use.
Source: http://drkoop.com/template.asp?page=newsdetail&ap=93&id=1504 313

19. *June 13, Taipei Times (Taiwan)* — **Researcher contracts dengue fever. The Taiwan Center for Disease Control (CDC) Saturday, June 12, said that a second person had contracted dengue fever in a laboratory, after the first case of dengue fever in Taiwan this year had been declared the result of laboratory mismanagement.** The center said that a graduate student doing research at a university in central Taiwan was confirmed to have contracted the disease on May 13. According to the CDC, the patient started showing symptoms on April 22. Because the student's research had been focused on Armigeres subalbatus, one of the most common mosquito species in Taiwan, the CDC requested in April that all lab work related to the dengue virus be discontinued and that lab safety checks be performed. The laboratory has since been closed down pending changes to safety regulations and operating procedures, the CDC said, adding that labs conducting research on invertebrates would in the future have to abide by strict World Health Organization regulations and guidelines. **The center's revelation**

follows close on the heels of a string of laboratory−related Severe Acute Respiratory Syndrome (SARS) cases in Singapore, China, and Taiwan. The infections all stemmed from contact with laboratory virus cultures, which gave rise to questions about the safety precautions at research laboratories handling infectious substances.
Source: http://www.taipeitimes.com/News/taiwan/archives/2004/06/13/2 003174853

20. *June 11, CIDRAP News* — **Bioterrorism guidebook for coroners. The U.S. Centers for Disease Control and Prevention (CDC) has published a guidebook to help medical examiners and coroners detect and respond to bioterrorism.** Besides providing detailed guidance for medical examiners and coroners, the report is designed to help other public health officials understand the role of medical examiners in bioterrorism preparedness and response. The document includes a description of the pathologic findings and diagnostic specimens and tests for each of the Category A (high−risk) bioterrorism agents: those that cause smallpox, anthrax, plague, tularemia, botulism, and viral hemorrhagic fevers. The guidebook includes information to help coroners cooperate with public health laboratories in the Laboratory Response Network, minimize the risk of infection when conducting autopsies, understand their role in surveillance for bioterrorism, and properly collect and document data from death investigations. **The report also includes a table linking pathologic syndromes seen on autopsy with potential terrorism−related illnesses, plus photos of tissue specimens from victims of diseases such as anthrax, plague, tularemia, smallpox, and Ebola.** The guide is available at http://www.cdc.gov/mmwr/preview/mmwrhtml/rr5308a1.htm.
Source: http://www.cidrap.umn.edu/cidrap/content/bt/bioprep/news/jun 1104examiners.html

[Return to top]

Government Sector

Nothing to report.
[Return to top]

Emergency Services Sector

21. *June 14, Firehouse.com* — **Disaster drill to be held on Ellis Island.** To prepare for the reopening of the Statue of Liberty this summer, federal authorities are holding a disaster drill on Ellis Island Monday, June 14. **The National Park Service, the Department of Homeland Security and the city's Office of Emergency Management will train some 50 workers to search for and rescue victims. They will also learn how to put out fires and give first aid under disaster conditions.** The Statue of Liberty, which has been closed to visitors since the September 11, 2001, attacks, is set to reopen by August, after safety and security upgrades. The island itself reopened three months after the terrorist attacks, but tourists have not been allowed inside the statue. When it reopens, visitors will only be able to tour the museum and take the elevator into the pedestal, and the stairs to Lady Liberty's crown will remain off−limits.
Source: http://cms.firehouse.com/content/article/article.jsp?section Id=46&id=31615

[Return to top]

Information Technology and Telecommunications Sector

22. *June 14, vnunet.com* — **Multilingual worm spreads throughout Europe.** A new multilingual worm from Hungary hit networks over the weekend and is spreading steadily. Zafi.B, also known as Erkez.b or Hazafi, spreads via peer−to−peer software and as a 12,800 byte .pif attachment within emails. **It has the potential to spread widely as it mails itself out in Hungarian, English, Italian, Spanish, Russian and Swedish.** Once activated the worm copies itself into the registry file and starts harvesting email addresses and mailing itself forward using its own SMTP engine. Zafi.B also terminates any application that has 'firewall' or 'virus' in its filename and several Windows tools, like Task Manager and Registry Editor. Its predecessor, Zafi.A, surfaced in April but had little impact outside Hungary as it only sent itself to .hu addresses. The motivation for the writer appears to be political in both cases. Zafi.B contains code urging the Hungarian government to accommodate the homeless and bring back the death penalty.
Source: http://www.vnunet.com/news/1155879

23. *June 14, Government Computer News* — **NIST releases security guidance on mapping information.** The National Institute of Standards and Technology (NIST) has released the final version of its guidelines for categorizing information housed in federal IT systems. The Federal Information Security Management Act (FISMA) requires agencies to identify categories of information they maintain and to assess the impact on the agency's mission of compromises to that information. NIST is charged with providing guidance on this and other FISMA requirements. The guidance is provided in Special Publication 800−60, Guide for Mapping Types of Information and Information Systems to Security Categories. Volume 1 of the document provides guidelines for identifying impact levels for violations of confidentiality, integrity or availability of a given type of information. Volume 2 includes examples of mission−based information types and suggests provisional impact levels. **The document focuses primarily on management and administrative information, which is likely to be common among many agencies, rather than on mission−specific information.**
Source: http://www.gcn.com/vol1_no1/daily−updates/26209−1.html

24. *June 14, Computerworld* — **Gartner sees growing need for wireless security policies.** The escalating use of wireless technology demands formal corporate security policies, according to users and analysts at a Gartner Inc. security conference in Washington, D.C., last week. This includes putting in place dedicated intrusion−detection systems for wireless networks, locking down wireless−enabled systems or installing personal firewalls on them, and keeping all wireless LANs outside the corporate firewall, they added. **Companies need to think beyond simply securing WLAN access points when looking at the security problems created by wireless use**, said John Pescatore, an analyst at Stamford, Conn.−based Gartner. Instead, the individual client devices inside a WLAN will pose the biggest security risks to corporations for the next several years, he said. Unprotected wireless client devices such as notebooks and handheld devices can be exploited as peers or access points to break into corporate WLANs where they can remain undetected indefinitely, Pescatore cautioned. **Concerns such as this have caused the International Monetary Fund (IMF) to put its entire WLAN outside the corporate firewall**, said Patrick Hinderdael, a division chief. The IMF is using virtual private network technology to authenticate users into its networks, and it's evaluating the option of putting all WLAN traffic in a segregated virtual LAN segment.

Source: http://www.computerworld.com/mobiletopics/mobile/handhelds/story/0,10801,93788,00.html

25. *June 11, SecurityFocus* — **Backdoor program gets backdoored.** The author of a free Trojan horse program favored by amateur computer intruders found himself with some explaining to do to the underground last month, after his users discovered he'd slipped a secret backdoor password into his popular malware, potentially allowing him to re−hack compromised hosts. The program in question is Optix Pro (Backdoor.OptixPro.12), a full−featured backdoor that allows an intruder to easily control a compromised Windows machine remotely, from accessing or changing files, to capturing a user's keystrokes or spying on a victim through their webcam. **The program has been downloaded nearly 270,000 times, according to a counter on the distribution site.** Optix Pro is a server that the hacker must insinuate into a victim's computer, either through subterfuge or by uploading it to an already−compromised machine. The hacker sets a password on the Optix Pro server, so that no other would−be intruders have the ability to slip through the open backdoor. That is, none except for the author, a coder named "Sleaze," who secretly embedded in the program a random−looking 38−character "master password" that was known only to him. **If the FBI ever got too close to Sleaze he had intended to release the secret password to the world, causing Optix Pro to become less popular among intruders and easing the pressure from law enforcement.**
Source: http://securityfocus.com/news/8893

Internet Alert Dashboard

DHS/US−CERT Watch Synopsis

Over the preceding 24 hours, there has been no cyber activity which constitutes an unusual and significant threat to Homeland Security, National Security, the Internet, or the Nation's critical infrastructures.

Watch Synopsis: We continue to receive reports of Korgo Worm Infections from both Public and Private organizations. Such reports indicate that not all organizations have successfully patched their networks for the LSASS vulnerability mentioned in Microsoft Bulletin MS04−011. Most infections in organizations have been traced to Insecure partner VPN connections to external organizations or infected laptops introduced into the network without prior verification that the systems were patched and virus−free.

Current Port Attacks

Top 10 Target Ports	80 (www), 1026 (nterm), 1080 (socks), 9898 (dabber), 3128 (squid−http), 1025 (blackjack), 1434 (ms−sql−m), 5554 (sasser−ftp), 135 (epmap), 1027 (icq) Source: http://isc.incidents.org/top10.html; Internet Storm Center

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Website: www.us−cert.gov.

Information on IT information sharing and analysis can be found at the IT ISAC (Information Sharing and Analysis Center) Website: https://www.it−isac.org/.

[Return to top]

General Sector

26. *June 14, Washington Post* — **Washington area builders find security is a keystone.** Since the September 11, 2001, terrorist attacks, putting up buildings in Washington for government departments or private government contractors has included an emphasis on security. At least one third of the 14 million square feet of office space now under construction in the Washington area is being built directly for government space or for a government contractor, according to Delta Associates, a Virginia real estate research firm. Background checks, escorts, X−ray scanning of trucks, even hiring only U.S. citizens so they can get required security clearances are routine for general contractors in the Washington area. **While many of the rules have been in place for years, most have been stringently followed only since the terrorist attacks, company officials say. The renewed emphasis has forced many construction companies, as well as other Washington area businesses, to change the way they hire and do business.** Security clearances are limited to citizens, and an increasing number of sites are requiring clearances at some point in a project, contractors say. That is no easy task for an industry dependent on immigrants and day laborers.
Source: http://www.washingtonpost.com/wp−dyn/articles/A38994−2004Jun 13.html

27. *June 14, Reuters* — **Somali charged with plotting to blow up mall. A Somali man living in Ohio was charged with plotting with al Qaeda supporters to blow up a shopping mall in Columbus, OH, Attorney General John Ashcroft said** on Monday, June 14. According to an indictment unsealed in Columbus, Nuradin Abdi attended a camp in Ethiopia for military−style training in "preparation for violent jihad." **Ashcroft said after receiving his training in Africa, Abdi returned to the United States and he and others "initiated a plot" to blow up a Columbus area shopping mall.** In the indictment handed up by a grand jury in Columbus, Abdi was charged with conspiracy to provide material support to al Qaeda and with obtaining and using fraudulent travel documents. Ashcroft would give no details on how far along the planning was for the planned attack on the mall.
Source: http://www.reuters.com/newsArticle.jhtml?type=topNews&storyI D=5417348

28. *June 13, Associated Press* — **Pakistan arrests al Qaeda suspects. Pakistani authorities have arrested 10 suspected al Qaeda members, including a nephew of detained terror mastermind Khalid Shaikh Mohammed, who has been in U.S. custody the past year, the interior minister said Sunday, June 13.** The men were arrested over the weekend in separate raids in the southern port city of Karachi, Interior Minister Faisal Saleh Hayat said. Among them was Masrab Arochi, a nephew of former al Qaeda number three Mohammed, who was captured in March 2003 in a city near the Pakistani capital. Arochi had a $1 million bounty on his head, Hayat said, and is believed to have been behind several attacks in Pakistan. **The interior minister said among those taken in were eight Central Asians who confessed to an attempt to assassinate Lt. Gen. Ahsan Saleem Hayat, the corps commander of Karachi. The general was unharmed, but 10 others died in the attack.** A tenth suspect arrested in the past 24 hours was identified as the mastermind of two sectarian attacks in the southwestern Pakistani city of Quetta in the past few months that left scores dead. Hayat did not reveal his name.
Source: http://apnews.myway.com/article/20040614/D836G7O80.html

[Return to top]

DHS/IAIP Products &Contact Information

The Department of Homeland Security's Information Analysis and Infrastructure Protection (IAIP) serves as a national critical infrastructure threat assessment, warning, vulnerability entity. The IAIP provides a range of bulletins and advisories of interest to information system security and professionals and those involved in protecting public and private infrastructures. By visiting the IAIP Web page (http://www.nipc.gov), one can quickly access any of the following DHS/IAIP products:

DHS/IAIP Alerts − Advisories and Information Bulletins: DHS/IAIP produces two levels of infrastructure warnings. Collectively, these threat warning products will be based on material that is significant, credible, timely, and that addresses cyber and/or infrastructure dimensions with possibly significant impact.

DHS/IAIP Daily Open Source Infrastructure Reports − The DHS/IAIP Daily Open Source Infrastructure Report is a daily [Monday through Friday] summary and assessment of open−source published information concerning significant critical infrastructure issues.

DHS/IAIP Daily Reports Archive − Access past DHS/IAIP Daily Open Source Infrastructure Reports.

DHS/IAIP Daily Open Source Infrastructure Report Contact Information

Content and Suggestions:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644.
Subscription and Distribution Information:	Send mail to dhsdailyadmin@mail.dhs.osis.gov or contact the DHS/IAIP Daily Report Team at (703) 883−3644 for more information.

Contact DHS/IAIP

To report physical infrastructure incidents or to request information, please contact the National Infrastructure Coordinating Center at nicc@dhs.gov or (202) 282−9201.

To report cyber infrastructure incidents or to request information, please contact US−CERT at soc@us−cert.gov or visit their Web page at www.us−cert.gov.

DHS/IAIP Disclaimer